REMARKS

Interview Summary

The Applicant would like to thank the Examiner for granting the interview on February 22, 2006, with Lisa Norton, Alan Schunemann and Chris O'Haver. The interview was very helpful. At the interview, Examiner Lin requested a summary explaining the arguments presented at the interview, which arguments are set forth below. Examiner Lin suggested amending the preambles of the independent claims to clarify the purpose of finding the relevant information, which the Applicant has done. He also suggested clarifying the language relating to determining which contacts are using the extracted Internet Protocol addresses, which the Applicant has also done.

Response to Office Action

In the Office Action, the Examiner objected to Claims 1-3, 5-9 and 31 because the term "the name discovery apparatus" in Claim 1 lacked antecedent basis. Applicant has changed "the" to "a" in Claim 1 in order to address the Examiner's objection.

In the Office Action, the Examiner indicated that Claims 1-3, 5-13, 15-16, 18-25, and 27-35 were rejected under 35 U.S.C. 103 as being unpatentable over Mukai (U.S. Pub. 20020178382).

Claims 1-3, 5-13, 15-16, 18-25, and 27-35 are pending. Claims 1, 10, and 22 are the independent claims. Claims 1, 10, and 22 are patentable over Mukai because these claims include the limitation that **the discovery apparatus discovers which contacts are currently using each of the extracted Internet Protocol (IP) addresses**. It is clear from Applicant's disclosure that the IP address is not already present in the organization's directory information, but **must be discovered** by the discovery apparatus. See, for example, page 5, lines 5-11 of Applicant's specification:

> In an embodiment, the present invention is provided to an enterprise as a solution for mapping Internet Protocol (IP) addresses to an organization's personnel using directory data and the contents of network traffic. First, the enterprise's local area network (e.g., Ethernet, FDDI or the like) traffic is captured and analyzed by installing a name discovery system apparatus (i.e., "NDS" hardware) on the primary switch of the enterprise's local area network (LAN). The captured data is cross-correlated with list data to map IP addresses to end users.

In contrast, **Mukai must manually compile a list of IP addresses** that are used by users in the organization's directory information. See, for example, FIGURES 7 and 15 of Mukai, which illustrate Mukai's **manually compiled** lists. Mukai does not discover this initial information by monitoring the network. Thus, Mukai's manually compiled list is subject to being outdated or incorrect, whereas Applicant's network-discovered list is much more accurate.

Claims 1, 10, and 22 are also patentable over Mukai because these claims include the limitation that a discovery apparatus must have at least one connection to a **switch** for passively monitoring traffic through the switch. In contrast, in Mukai, **hubs** are used to see network traffic. With Mukai, **when a switch** (i.e., switching hub) **is used**, Mukai is not able to see the network traffic, and communication monitor software must be installed at each device to be monitored in order to see that device's traffic. Specifically, paragraph 0250 of Mukai states:

> The security administration server S collects the communication packets flowing in the LAN by the following methods. For example, regarding communication packets transmitted and received by the device to be monitored C connected to a same hub as the security administration server S, they may be directly obtained by the server S itself and the server S directly obtains them (however, excluding a case where the hub which the security administration server S is connected to has an intelligent function like as a switching hub). On the other hand, when the server S itself is connected to a switching hub, or regarding communication packets transmitted and received by a device to be monitored C which is connected to a hub different from the hub the server S is connected to, the server S itself cannot directly obtain them. Regarding the communications packets, for example, a program to obtain the communications packets (communications monitor software) is operated at the device to be monitored C side, and with an effect from this program, the communication packets accumulated and stored in the device to

be monitored C are concentrated to the security administration server S at a suitable timing via the LAN, to be obtained.

For the above reasons, independent Claims 1, 10, and 22 are allowable. The remaining claims depend, either directly or indirectly on Claims 1, 10, or 22, and are thus also allowable.

Applicant believes that a full and complete reply has now been made to the Office Action and, as such, the present application is in condition for allowance. The Examiner is invited to contact the undersigned by telephone should the Examiner believe that personal communication will expedite prosecution of this application.

Respectfully submitted,

DLA PIPER RUDNICK GRAY CARY U.S. LLP

Dale Lazar
Registration No. 28,872

Lisa K. Norton
Registration No. 44,977

P.O. Box 9271
Reston, VA 20195-3171
(703) 773-4149 Telephone
(703) 773-5064 Facsimile